EMGT 835 FIELD PROJECT:
Information Security Framework for Small and Medium Sized Businesses

By

Steven M. Michnick

Master of Science

The University of Kansas

Spring Semester, 2006

An EMGT Field Project report submitted to the Engineering Management Program and the Faculty of the Graduate School of The University of Kansas in partial fulfillment of the requirements for the degree of Master of Science.

Herb Tuttle **Date**
Committee Chair

Chick Keller **Date**
Committee Member

Annette Tetmeyer **Date**
Committee Member

Table of Contents

Acknowledgements

I want to thank the EMGT Faculty for the wonderful learning opportunities I experienced as part of the EMGT program. I especially would like to thank the members of my field project committee, Prof. Herb Tuttle, Prof. Chick Keller, and Annette Tetmeyer for their patience and help in completing this field project. None of this would be possible without thanking my mother and father for their support and encouragement all along the way towards my Master's degree. They have been there for me when life's challenges made me feel like stopping and encouraged me to keep going. Finally, I would like to thank Marci Wright for her support and patient proofreads of my field project. Marci, you inspired me to finish this project and I hope you will continue to inspire me towards other accomplishments throughout my life. It means very much to have your encouragement and support. I look forward to sharing so much more of my life with you.

Corrections

I was informed in June 2009 of an incorrect attribution of the information in Table 1 to McGill University, Network and Communications Services in the original version of this Field Project. The correct author of the information on page 22 in Table 1 is George Shaffer of GeodSoft.com. McGill University, Network and Communications Services had done additional research based on Mr. Shaffer's original work but that research is no longer available from McGill University, Network and Communications Services.

I have corrected the reference and updated the information in Table 1 and the preceding paragraph on page 22 with the revised work that Mr. Shaffer did in April 2007 and is published on the Geodsoft.com web page.

http://geodsoft.com/howto/password/cracking_passwords.htm

I regret the attribution error and appreciate Mr. Shaffer's understanding in bringing the matter to my attention.

Executive Summary

Information security issues are a challenge to everyone who uses computers. The rise of the personal computer as a common business tool and the Internet as a common means of business communication and commerce have also created an environment that criminals with technical knowledge can exploit to prey upon the less technically savvy. The cost of computer crime to business in the United States has risen to $67 billion according to the 2005 FBI Computer Crime Survey. Not a day goes by that a computer security exploit or identity theft scheme makes national headlines. The impact to small and medium sized businesses is tremendous. These businesses have the least amount of resources to use to help defend against hacker attacks and they suffer some of the largest net financial impacts when victimized by an attack.

The good news is that there are some simple things a business owner can do to greatly reduce the risks of being victimized by an information security failure. Education and awareness of the most prevalent risks to business information and commonly exploited security holes can quickly close the door to a security incident. Just as with traditional burglary attempts, the computer criminals will first look for the path of least resistance when trying to break in to a computer system. If a door is unlocked, all the criminal has to do is walk right in. The problem with computer technology is that many people do not even know when the doors are unlocked.

By raising awareness of the most common vectors of attacks against business computer systems, this field project seeks to help business owners better manage and protect their information assets. The computer risks and mitigation approaches outlined in this project will not completely eliminate all the computer security exposures that

company can face in the 21st century business environment but they will help a business owner know what they can do to quickly reduce their risk exposure. Just like with any other type of crime, a determined criminal may eventually find some type of security weakness that can be exploited for illicit purposes. The goal of the business owner is to make the criminal's work so hard that they look elsewhere to commit their crimes.

Introduction

Information Technology (IT) has permeated every sector of the United States economy. The introduction of the IBM Personal Computer (PC) in 1982 and the rapid acceptance of the Internet since 1992 by businesses and household users fueled one of the largest expansions in the history of the U.S. economy. The resulting impact of the Internet Technology Revolution on small businesses has been tremendous and both a boon and bane. In a few short years, small business owners have needed to become familiar and adept with computer technology to take advantage of new business opportunities and to match competitors. For many people, computer technology is very complicated and they simply take the path of least resistance to get a computer system up and running. Unfortunately, the quick and easy path might get the system up and running but keeping the system running is an entirely different matter. This leads to significant exposure to risks that a business can ill afford. Small and medium sized business (SMB) owners are confronted with the same set of information security issues as billion dollar corporations, and the SMB owners do not have deep pockets to pay for solutions. The end result is that the largest portion of the U.S. economy is running at the highest exposure to Information Security problems

Most SMB owners know all too well the headaches created by system crashes, data loss, and virus attacks. The bad news for anyone who uses computers and the Internet is that information security threats are some of the fastest changing aspects of Information technology. There are literally hundreds of new virus and worm attacks appearing weekly. Protecting the privacy of customer and client information is more important than ever with identity theft being one of the fastest growing crimes in the

world. Complying with new federal and state regulations is enough to make SMB owners simply want to turn all their computers off.

Many business owners are overwhelmed and feel they must become IT specialists just to keep their computers running their business. They are stuck in a quandary, they cannot operate without the computers, but they cannot spend all of their resources just trying to keep them working without risk. The risk is real because it only takes a few days of down-time to lose thousands of dollars in revenue. It only takes one incident of losing customer private information to irreparably damage a business' reputation. One bad security event has the potential to put someone completely out of business.

A business owner needs a framework that will help to understand the different types of risks that different technical components bring to the table. The business owner does not need to become an IT professional but they need assistance to help them communicate effectively with IT support and to evaluate if the support is doing their job. They also need a guide to help them find the most cost-effective approaches to mitigating IT security risks. The good news is that there are truly some very good free or relatively inexpensive software solutions that can assist in making business computer systems secure. The challenge for SMB owners is to quickly understand the areas of risk and what software packages can help to mitigate it. This field project aims at creating a framework that can successfully serve as a guide for informing a business owner of the risks and how to implement a solid IT security discipline for computer systems with access to the world wide computer network that provides sound computer and network security today and tomorrow.

The Statistics of U.S. Small Businesses

It may seem surprising to most people, but small businesses of fewer than 500 employees represent a majority of the employers in the United States. The Small Business Association's Office of Advocacy reports the following statistics for 2002 (the latest year with data available) Small businesses:

- Represent 99.7 % of all U.S. employers
- Employ 50% of the U.S. private work force
- Employ 38% of the private workers in high-tech occupations
- Provide 51% of the private sector output
- Represent 96% of all exporters of goods
- Receive 35% of federal contract dollars
- Are home-based 53% of the time and are franchises 3% of the time
- Provide virtually all of the net new jobs

(Source: SCORE, Counselors to America's Small Business, www.score.org and Small Business Administration Office of Advocacy, www.sba.gov)

Theses statistics reveal that small businesses are the lifeblood of the U.S. economy. Even though big corporations represent about 80 percent of the total sales revenue, most of those sales are to other large corporations.

At the same time it is these same small businesses that are the least aware of Information Security issues and consistently fail the basic tests that demonstrate their Information Assets are adequately protected. To demonstrate the depths of this problem, consider the impact of the outbreak of the "Melissa" email virus in March 1999. This outbreak was the first major virus outbreak to affect business in the matter of a few days.

The estimated cost of Melissa to U.S. businesses currently stands at $80 million. This outbreak opened many eyes to one of the major risks implicit with the use of information technology. However, this exercise did not appear to do much with regard to prevention because a little more than one year later on May 4, 2000, the “I Love You” email worm hit the Internet and by May 8, 2000 had infected more than 45 million computers. The current estimated costs of the “I Love You” bug to U.S. businesses stands at $10 billion. Any business owner who experienced the loss of system availability and the subsequent clean up work from any of these events began to understand that more must be done to mitigate the serious threat that computer viruses and worms pose to their business. Yet, the lessons don’t appear to stick very well. In 2001, the “Code Red I and II” worms appeared and cost businesses $2.6 billion. That same year the “Nimda” virus appeared costing up to an estimated $2 billion. In 2002, the “Klez” worm struck, taking a hefty $9 billion bite out of businesses. The list continues to the present with the recent attack of the Zotob worm on August 16, 2005, and begs the question, “Are the viruses and worm writers just getting smarter, or is IT management missing something in their approach to defending against these attacks?” The truth is that both are to blame. The derelict programmers who create these evil bits of code are constantly finding new ways to create havoc, but there is more business owners can do to thwart them at every turn.

The issue of information security is not limited to just computer virus attacks. Information security covers a wide range of computer issues that present risk and liability to a business that uses information technology. This project is an effort to build an Information Security Framework consisting of approaches and policies that address the following Information Security issues:

- Information Access Policies
- Malware Protection
- Network Protection
- Information Backup and Recovery Strategies

Literature Review

Information Security is a highly dynamic and rapidly changing field with a very diverse range of sources for security issues and best practices. It is a subject matter that deals with an "arms race" between criminal hackers and computer professionals. The hackers are always looking for a new chink in the IT armor to exploit. There are numerous books available that focus on information security practices for businesses but because the subject is very dynamic they quickly become outdated within a few years of publication. These books outline a core methodology of security practices but the technical implementation information becomes outdated within two or three years of publication due to advances in technology and changes in security threats. Engineering textbooks such as "The National Computer Security Association's Guide to Enterprise Security" by Dr. Michel E. Kabay, published in 1996, provide very good introduction to information security problems and methods to mitigate their risks. Dr. Kabay's book provides a good summary of computer virus attacks that occurred prior to 1996 but offers no information relevant to preventing an email virus attack like the "I Love You Virus" of 2000. The 2003 edition of Security in Computing by Charles P. and Shari L. Pfleeger, is another example of a text that offers good information security theory at a general level and is useful in helping to formulate policies but suffers from age at only three years old. It does not describe the threats from "phishing" attacks where a criminal sets up a website that masquerades as a company's real site with the hope of duping customers to input their personal information. Phishing attacks began appearing around 2003. The Pfleeger's text also does not cover the problems of spyware and adware in their sections dealing with software security even though this problem began impacting businesses in 2001.

The newest book reviewed by Mark Stamp called, “Information Security: Principles and Practice,” directly addresses the topic of information security. It provides a very thorough discussion of cryptography, access control, security protocols, and software security issues. The cryptography section provides a solid basic introduction and then detailed chapters on symmetric key, public key, hash functions, and advanced cryptanalysis. Most of these details are beyond the scope of this field project but the text does serve as a good reference for anyone needing explicit information about cryptography. The Access Control section provides excellent, up-to-date, information regarding problems with passwords, two-factor authentication methods, and biometrics. Again the book goes into details beyond the scope of this field project but would serve as an excellent guide for implementing a state-of-the-art authentication, authorization, and accounting (AAA) system. The software section summarizes the current software flaws that are commonly exploited by viruses and worms. It also covers techniques that can be used to analyze software for security weaknesses and discusses operating system security functions.

The most current and pertinent information available on information security practices for businesses appear in publications from organizations focusing on computer security like Information Systems Security Association (ISSA), the SANS (SysAdmin, Audit, Network, Security) Institute, and the USENIX Association and their associated Internet web sites. Also important computer security practices and news of security challenges facing businesses can be found in IT trade journals such as CSO magazine, PC Magazine, Infoworld and their associated Internet web sites. These security organizations’ publications and IT trade journals provide a constant stream of timely

information about the latest computer security threats and technical details on mitigating these threats. These sources reflect the current state of the battle between criminal hackers and the businesses they prey upon. Business owners interested in protecting their information assets should pay interest to these sources of information to keep their information security efforts up to date.

The SANS Institute provides some excellent, freely available resources that explain the reasons for and how to rapidly implement solid Information Security Policies. This information can be found at http://www.sans.org/resources/policies/.

The United States Computer Emergency Readiness Team (US-CERT) and the Carnegie Mellon Software Engineering Institute CERT Coordination Center together provide excellent resources for obtaining the most current about the information security threats. They also provide detailed histories about computer malware along with steps to follow for removing infections and mitigating exposures to attacks. This information is available from their websites at http://www.us-cert.gov/ and http://www.cert.org/.

The Computer Security Resource Center at the U.S. National Institute of Standards and Technology offers information and workshops that are specifically designed to address information security issues of small businesses. NIST is a world leader in guidelines for securing information assets. This information is available at http://csrc.nist.gov/securebiz/.

Information Access: Locking the Front Door to Computers

Information Access Policies

The cornerstone of a good Information Security Framework begins with Information Access and Security Policies. Information Technologists commonly refer to these as Authentication, Authorization and Accounting (AAA) policies. These policies address what people must do to authenticate, i.e. prove who they are to a computer system, manage which computer systems they are authorized to use, and the procedures that must be followed to keep track of what they do on the computer system to account that the information stays secure. These policies cannot in themselves make the computer systems and networks completely secure-- no set of policies can achieve that-- but they can limit the exposure to risk and raise awareness regarding the most common approaches taken by people bent on breaching computer access security. These policies do not need to be complicated; in fact, the opposite should be true for the policies to be easily understood. It may seem like overkill for a very small business with only two or three people to have a set of written Information Access and Security Polices, but even in this situation they can serve as point of agreement and be incorporated into legal documents defining a partnership. In order for these policies to work they require the complete backing and support of the business management, starting with the president or CEO, otherwise they become useless. In short, the business manager must enforce the policies and give them teeth.

Acceptable Use Policy

An ideal starting point for establishing Information Access Policies is an Acceptable Use of Computer Systems policy. This policy sets the tone and outlines for all company employees what can and cannot be done with computer systems. This policy establishes the responsibilities of everyone who uses business computers. Accessing, creating, and modifying business information requires that employees understand the responsibilities they incur for keeping this information secure. Also, most business managers are concerned with employee productivity and this policy is an appropriate place to address the issues of using computers for non-business related activities such as game playing and inappropriate web surfing on the Internet. The purpose is to educate employees that by using company computers they are legally bound by the company's rules of usage and that their usage of the computers can and will be monitored. Many Acceptable Use Policies in place at major corporations strive to maintain flexibility so that incidental personal usage of computers is accepted but informs the employee that company maintains the right to determine what "incidental" usage is. The Acceptable Usage Policy typically includes language delineating:

- Systems that employees may or may not use
- Permissible hardware changes an employee may make
- Software installation and removal allowed by employees
- System configuration changes an employee may make such as modifying boot-up sequence
- The type of work an employee can use on a computer, i.e. conducting personal business or modifying sensitive data

The first step to establishing an Acceptable Usage Policy is to understand that a business needs one, and then the next step is to designate someone in the business to be responsible for the development, maintenance, and enforcement of the policy. Depending on the size of the organization this person should be a partner, a senior manager, or someone with appropriate authority to enforce the policy. It is advisable to separate this responsibility from system administrators and other technical staff as they typically do not have the authority needed to effectively enforce the policy.

With someone in authority appointed as responsible for the Acceptable Use Policy, they should work to develop the policy with stakeholders from across the organization. Stakeholders should include key personnel from all areas who use computer systems, especially the system administrators. This provides input regarding how aspects of the policy could affect the performance of job duties. While business management is responsible for establishing and enforcing the usage policy, it is extremely important to include input from staff that uses the computer systems and the people who must maintain the systems.

When the policy is finally drafted the next challenge is to present it to everyone in the organization in a manner that clearly explains the motivation for the policy and the consequences for not complying with it. At this point the stakeholders who worked to develop the policy can help to communicate the policy's message to their peers. It is very important to document acknowledgement by all employees that they understand the Acceptable Usage Policy and agree to follow it. This puts the policy into action. The final component of implementing the Acceptable Usage Policy is to place a statement that all employees see each time they login in to a computer which reiterates that they must use

the computer in accordance with the policy and that the computer may be monitored for compliance. This helps remind the users of their responsibilities and limits the risks of liability and litigation. A periodic review and update of the policy is necessary to accommodate changes in technology, threat events, and legal responsibilities.

Included as Appendix I is a sample Acceptable Usage policy available from The SANS Institute, a highly regarded computer security policy group serving over 165,000 computer professionals from academia, government, and industry.

Password Policy

An adjunct to the Acceptable Usage Policy as part of the Information Access Policies is a Password Policy. The Password Policy describes the rules for creating, updating, and protecting the passwords used to access company computers. The fundamental components of a password policy address the factors of password length, use of common words, character mixture, and aging requirements. Defining the password policy is the easy part; the real challenge for business management comes down to enforcing it. Passwords are the most heavily relied upon form of security protecting computers from unauthorized access and by their very nature, as the keys to sensitive data, the ultimate goal of computer hackers is to discover them. The average computer user of today is required to remember several passwords and with systems that are constantly forcing a user to update passwords for security reasons it is easy to see how a user can become quickly frustrated and abandon good password security practices. This problem makes user authentication one of the weakest fronts in the battle for computer security so it is critical for business owners to understand risks that result from a compromised password and the methods attackers often use to discover passwords.

There are four key categories of abuse that can arise from a comprised password; Identity Theft, Sensitive Data exposure, Company Data exposure, and Criminal Intent. Identity Theft is defined as acquiring and using personal or business identification data, such as social security numbers or business tax numbers, to fraudulently obtain lines of credit to purchase goods or services with no intention of paying the bills. Identity theft has been widely publicized by the media due to the rapid rise in the number of serious cases. According to Federal Trade Commission estimates, identity theft affected 10 million Americans causing consumer losses of $2.4 billion and costing businesses $48 billion in 2004 (Zeller, NY Times, 2005). Identity Theft will seriously impact a business' credit ratings resulting in difficulty in raising capital and obtaining legitimate lines of credit.

Sensitive Data Exposure is defined as a breach of security that would give unauthorized persons access to email, personal documents and pictures, and personal project information. This scenario can easily enhance a criminal's efforts to hijack someone's personal digital identity for the purpose of furthering their attack on the company or for possible extortion against the individual.

Company Data Exposure is a security breach that results in unauthorized access to company data files. This type of exposure can lead to the loss of trade secrets, financial data, sensitive client information, and other types of data that in the wrong hands could jeopardize the business' viability.

The last category, Criminal Intent, is specifically defined as a breach in security that allows someone to use company computers and networks as a staging ground and cover for any variety of criminal activities, other than Identity Theft. Examples include,

but are not limited to, running file servers to trade illegal copies of software and other copyrighted materials, running web servers to supply illicit pornography, and mail servers to send out unsolicited emails. Any sort of criminal activities that occur on company computer systems expose the business to unlimited liabilities and when publicized will seriously damage the business' reputation.

There are five common scenarios that can lead to compromising a password which a business owner needs to understand (Danchev, WindowSecurity.com, 2005).

1. Physical Security Breach – This is the most critical situation and occurs when someone completely bypasses all authentication methods to obtain data. One typical type of physical security breach is due to theft of computer hardware. This gives the criminal all the time they need to scan the computer hard disk for any information that they might find useful to further compromise company systems and exploit company information. Another common type of physical security breach occurs through the installation of keylogging software or hardware on the computer. Keyloggers track all the keystrokes typed on the computer's keyboard. The log of keystrokes is then examined to discover passwords and other information that should remain secure. Keylogging software can be installed by someone with legitimate access to the computer system that has the intent to discover another user's passwords in order to masquerade as that user. Keylogging software can also arrive as part of a Trojan horse program, a type of computer program that appears innocuous and misleads the person into installing it so it can serve its true purpose of logging keystrokes. Trojan horse programs will be described in greater detail in the Malware section of this field project. In

either case all it takes to reveal someone's password is a look at the keylog file after that person has logged on to the computer system. It should be easy to see that keylogging can quickly circumvent all company computer security efforts to protect passwords. The best way to mediate the threat of someone purposely or inadvertently installing a keylogging program is to set the computer systems so that only administrative user accounts can install programs. The difference between administrative and regular user accounts is that the administrative account has special privileges that will allow modification of system configuration. Regular user accounts are limited to only running the programs they are authorized to use and only creating, modifying, and deleting files that are required for the user to conduct business.

2. Guessing – Most computer users do not like complicated passwords so they often pick one that is easy to remember such as the name of a spouse, friend, or a pet. A person wishing to access a computer using another person's account simply has to know some personal information to try and guess the password. This is why simple passwords that are based on personal information are very weak.
3. Cracking –There are numerous programs available on the Internet that support attempts to crack passwords by trying to decrypt the file used by the operating system (OS) to store passwords or mimic the process the OS uses to authenticate the user. Either way, if an attacker can gain access to the OS password file they can begin the process of trying to crack it and discover the contents. The key defenses against attempts at cracking password files are to make certain that the password is file only accessible by computer administrators. In the case of

computer theft the only defense is making sure a strong password policy is in place so that password cracking efforts take impossibly long periods of time, even with the fastest computers. A strong password is made up of a minimum of eight characters and includes uppercase letters, numerals, and special keyboard characters. Even with the fastest computer processors currently available, passwords of this type can take over 1000 years of computer processing time to crack by the brute force method of trying every possible combination.

4. Sniffing – Anytime a user sends a password across a network, especially an open network like the Internet, they run the risk of someone with access to network packet capturing capability catching the password. Originally the password authentication programs did not take into consideration that they might be used across an open network so there was no attempt to encrypt passwords. A user that logs on to a system across a network would send the password in a clear text format, one that is easily read by anyone who might be sniffing the packets passing through the network. To mitigate this situation there are now password authentication programs that use encryption, such as Secure Sockets Layer, for all network traffic. A business owner should require that all network traffic that will send a password encryption be encrypted even if it is a closed network. This eliminates the possibility of anyone ever using network sniffing to determine a password.
5. Sharing –When user accounts are shared by more than one person they may believe they are simplifying access to data used by multiple people. One of the most common tactics used by people bent on accessing private data is to simply

ask for access. Social engineering, discussed in detail in a following section of this field project, is the process by which an attacker works to gain the trust of an employee for the purpose of gaining physical and/or system access to company information. By sharing passwords to accounts, management loses the ability to account for who precisely is accessing company data. Accountability is critical to maintaining data integrity and many State and Federal regulations require it, this is why sharing passwords must be discouraged.

These five scenarios highlight the major weaknesses in passwords exploited by hacker's seeking to compromise a company's computer system.

The most common mistake computer users make is to use a common word found in a dictionary. Numerous password crackers are widely available on the Internet, such as PCL and L0phtCrack for Windows, and crack for UNIX and Linux, that focus on using brute force attacks against computer accounts by running through all words found in dictionaries for most common languages. In short, if it is a word in English, French, Spanish, German, or any other major spoken language it would not take long for a hacker armed with a brute force password cracker and a very large dictionary file to attempt every word in the file as a password. All the hacker needs is access to the user authentication prompt and sufficient time to scan through the dictionary. This is why a strong password policy must be enforced. Major computer operating systems, such as Windows and UNIX, come complete with features that a system administrator can turn on to enforce password length, character mixture, and aging requirements. One of the primary goals of a password policy is to specify the characteristics of a good, strong password. The password standard set forth by the SANS Institute and which is widely

accepted by computer security professionals is that a password must be eight characters long, contain a mixture of upper and lower case alphabet characters, and must include at least one numeric character and one special character from the available ASCII character set. This standard generates a very large number of possible character combinations since there are 26 lower case, 26 upper case, 10 numeric, 32 special characters, and the SPACE key character, which is valid for use in many password systems. This results in 95^8 or 6,634,204,312,890,625 possible character combinations for a password. Even with a computer capable of trying 1,000,000 password combinations per second, it would take almost 2,000 years to try every possible combination of an eight-character password with 95 character possibilities. Obviously, the password must contain a complete mixture otherwise the number of combinations and computing speed needed to try all of them quickly drops as is shown in Table 1 (George Shaffer, GeodSoft.com, Good and Bad Passwords How-to, 2007).

	26 characters	36 characters	52 characters	69 characters	95 characters
Password Length	Time to process	Time to process	Time to process	Time to process	Time to process
3	0.02 seconds	4.7 seconds	0.14 seconds	0.33 seconds	0.86 seconds
4	0.46 seconds	1.68 seconds	7.31 seconds	22.7 seconds	1.36 minutes
5	11.9 seconds	1.01 minutes	6.34 minutes	26.1 minutes	2.15 hours
6	5.15 minutes	36.3 minutes	5.59 hours	1.25 days	8.51 days
7	2.23 hours	21.8 hours	11.9 days	2.83 months	2.21 years
8	2.42 days	1.07 months	1.70 years	16.3 years	2.10 centuries
9	2.07 months	3.22 years	88.2 years	1.12 millennia	20 millennia
10	4.48 years	1.16 centuries	4.58 millennia	77.6 millennia	1,899 millennia
11	1.16 centuries	4.17 millennia	238 millennia	5,352 millennia	180,365 millennia
12	3.03 millennia	150 millennia	12,395 millennia	369,303 millennia	17,184,705 millennia
13	78.7 millennia	5,410 millennia	644,521 millennia	25,481,886 millennia	1,627,797,068 millennia
14	2,046 millennia	194,728 millennia	33,515,076 millennia	1,758,250,151 millennia	154,640,721,434 millennia

Table 1 - Brute Force Password Cracking Times

(George Shaffer, GeodSoft.com, Good and Bad Passwords How-to, 2007)

The a sample Password Policy available from The SANS Institute as shown in Appendix II is a good guideline for business owners to follow in assessing their computer systems native ability to enforce password length, character mixture, and aging requirements.

Alternatives to Passwords

Even with a sound password policy in place there is an inherent problem with having passwords serve as the primary means of preventing unauthorized computer access. According to Moore's Law, computer processor speeds will double every two years which drives the time to crack complicated passwords down to more realistic timeframes. Hackers have taken to assembling armies of processors to help further reduce the time it takes to run brute-force cracks against a complex password. Nothing can stop a compromised password so if the business owner truly wishes to eliminate the single factor authentication problem of passwords they need to turn to other methods.

Two-Factor Authentication

One method that eliminates many of the problems of using only a username and password for authorizing a computer user is two-factor authentication. This method works by requiring the person requesting authentication to know something and to have something. The user still must know a password and this password should still follow sound password policy. The security enhancement comes from the second component; the thing they must have. In early implementations of two-factor authentication the user had a physical key that they inserted into the computer system they were attempting to access. Modern implementations typically use an electronic token card that displays a randomly generated number. This random number generation is synchronized with the

system the user is attempting to log into and when they match, the user is granted access. RSA Security's SecurID is a very popular commercially available two-factor authentication product that can easily be implemented in small and medium-sized business computer environments.

Biometrics

Another approach to mitigating the problems with using passwords is biometric authentication. This method is based on personal physical characteristics and employs scanning of fingerprints, retina scans, voice recognition, face recognition or some other method of examining a unique personal characteristic to authenticate the user. This method still seems futuristic to many business owners and the expense of these systems can make them cost prohibitive. Yet if the risks of an information security breach are very high, then a biometric authentication system may be justifiable. The biggest challenge in trying to implement a biometric authentication system is to find one that is quick and easy to use. The system must be able to discriminate users in a non-intrusive way while minimizing false rejections and virtually eliminating false acceptances. False rejections are when the biometric system does not correctly identify a person with access authorization and false acceptances are when the system allows access to someone who does not have authorization. A study published in 2001, by Dr. Tony Mansfield, evaluated a variety of commercially available biometric authentication systems at United Kingdom's National Physical Laboratories and determined that false rejections were typically due to user error and unfamiliarity with the system. The study also concluded that there are several factors business manager's should consider before deciding to use a biometric system. The primary management decision factors include the required level of

system security along with the achievable accuracy and efficiency of a biometric system. The study also points out that factors such as health and safety of users, user acceptance, privacy, and legal issues should also be considered. All these factors affect the total cost and success of implementing and operating the biometric system (Mansfield, 2001).

Social Engineering

No matter what type of authentication process or access policies are in place, the weakest links in an organization's information security are the people that interact with the systems and follow the policies. Criminals understand this and constantly are looking for ways to subvert the authentication process and access policies by manipulating employees into giving away vital information that can help them gain unauthorized access to business information systems. These efforts are commonly called social engineering attacks and they can take a variety of forms, with the ultimate goal of gaining access to a valuable business system and the information it stores. Social engineering was the main approach used by Kevin Mitnick, an infamous computer hacker who broke into computers at Sun Microsystems, Nokia, Motorola, and Digital Equipment Corporation, just to name some of his largest corporate victims. Once a criminal like Mitnick gains enough access they can begin committing fraud, stealing identities, conducting business espionage, and create a general disruption of business activity. This makes protecting against social engineering attacks one of the most important areas of focus in information security.

Criminal hackers conducting social engineering attacks will work on physical and psychological levels. On the physical level, they will test building security by looking for open doors to facilities and enter pretending to be a salesperson, maintenance worker, or

consultant. Once inside they will scour the premises looking for any useful pieces of information that might further their attack. A company phonebook or a rolodex containing client contacts can be very useful aiding a criminal in their effort to understand the company's organizational structure and business agenda. A few nights spent rummaging through trash dumpsters can provide a wealth of documents with more details about business activities. The phone is a powerful tool for a skilled social engineer. On the psychological level, a hacker will work on a person's trust, emotions, and desires to gain information that will help gain access to company computer systems and information. Psychological attacks can range from simple requests for help from a seemingly needy individual, to seduction and extortion. Criminals, using some basic company knowledge, can easily operate on the psychological level by sounding as a confident individual or leveraging fear of a bad performance evaluation to gain enough of the employee's trust so they reveal critical system information that will help further the criminal's attack on the company. Seduction has been used on more than one occasion to co-opt passwords and access codes. The story of Susan Headley, a.k.a. "Susy Thunder", a high school dropout, prostitute, and associate of Kevin Mitnick, is legendary among hackers because she slept with military officers to obtain passcodes (Kabay, 1996). The Russian Mafia is also known to use extortion and violence to extract information that they can use to hack into computer systems (Scambray, 2001).

A common approach for a social engineering attack is a phone call to a company employee by someone imitating a technician or a person in authority. During the call they present a situation that requires the employee to provide passwords, IP addresses or other valuable company information. Most employees will try to be very cooperative when

they believe they are assisting a company official who is in desperate need of access to a computer system or believe they are helping a technician complete a task. Email also serves as a simple line of attack for social engineering. Emails that appear to be from a company official can also dupe unwitting employees to open an attached virus, worm, or Trojan horse that exploits a computer software defect. By executing the attachment the employee could open a backdoor to system access, start a process that erases data from hard drives, or begin the spread of the virus or worm to other computers on the network creating a company-wide denial of computer service.

An advanced method of gaining access to company information is called, “reverse social engineering.” This method works by creating a persona that employees seek out for assistance with computer problems or for other types of information. This type of attack can be very complicated to achieve and requires careful planning and execution in order to establish confidence and credibility as a source of knowledge. However, if done well, the hacker can gain access to larger volumes of company data than through traditional social engineering methods. A widely cited paper by Rick Nelson entitled, “Methods of Hacking: Social Engineering,” describes reverse social engineering as following three steps: sabotage, advertising, and assisting. The first step in this scheme is for the hacker to gain enough access to corrupt a system or at least, create the appearance of a corruption. Upon seeing the malfunction, the computer user will seek help, and by no simple matter of good fortune, the user ends up calling the hacker to help fix the problem. At this point, the hacker has gained the user’s confidence and system access to begin “fixing” the problem (Nelson, 2006).

The varieties of scenarios that these forms of social engineering attacks can create are numerous, with all of them resulting in compromises to information security that can be very difficult to fix. And it all starts with persuading someone on the inside to be all too trusting. This means that a business owner must constantly be vigilant and work to raise the awareness of employees about how social engineering attacks operate.

Training employees about security issues must be a constant effort and requires presenting information about the physical and psychological approaches criminals will pursue to break into the company. Employees need to be taught to be suspicious and to never divulge passwords and other revealing information about a company's computer system to anyone calling them on the phone or contacting them through email. This level of training is useful to the employees because it also applies directly in their personal lives to help protect them from identity theft and attempts to gain personal financial information. Employees should be trained on how to spot social engineering attacks. They should look for things that are not familiar and don't quite make sense. If a caller refuses to give contact information, tries to drop names to intimidate, makes spelling mistakes, or asks strange questions, then the employee should be suspicious and contact their manager immediately. It helps to think like a hacker to defeat hacker methods.

Training employees about physical security issues is also a requirement. Management must provide paper shredders or subscribe to a document destruction service to prevent valuable company information from leaking out through the trash. Employees must be required to use the shredders or locked disposal bins for all company documents. Physical security training must also emphasize building access policy. All guests must sign in and be accompanied by an employee. Employees cannot allow "tail

gaters” to follow them into locked facilities without proper company identification. Technology equipment, such as phone switches, network routers and computer servers, must be kept in locked areas with strictly limited access. Equipment inventories need to be constantly kept up-to-date and audits need to occur at regular timeframes, preferably at quarterly intervals. The audits should not be announced across the company and only the technicians performing the audits and key company officials should know when they occur.

Kevin Mitnick stated in his article, “My First RSA Conference,” that, “You could spend a fortune purchasing technology and services from every exhibitor, speaker and sponsor at the RSA Conference, and your network infrastructure could still remain vulnerable to old-fashioned manipulation (Mitnick, 2004).” His point should not go unheeded by anyone who has responsibility for information security and a company’s livelihood.

Malware Protection: Defending Against Viruses, Worms, Spyware, and Trojan Horses

The most prevalent information security threat in the minds of many people is an attack from a computer virus. These tiny programs and their nasty cousins; worms, spyware, and Trojan horses are truly the bane of modern computing. The damage they inflict and the additional costs they create for business is measured in the billions of dollars. Malware attacks are constantly changing to exploit newly discovered exploits in operating systems and commonly used programs like word processors and spreadsheet software. The newest form of malware; spyware and adware, works to capture sensitive information, such as userids, passwords, bank account numbers, and Internet usage patterns, so it can be sent to a secretive collection system for analysis by criminal hackers. Malware authors are constantly changing their approaches by blending the attack vectors and consequences of infecting a computer system. The traditional definitions of virus, worm, Trojan horse, and spyware apply mainly to describe the infection mechanisms and consequences but it is important to understand that new forms of attacks are created that blend these mechanisms to circumvent common protection approaches and cause a variety on negative consequences to infected computers.

Malware Definitions

A *computer virus* is a malicious program that copies itself into a host program or into special executable areas of a disk that are run during system boot time. When the virus infects the host program it can begin to subvert the normal program operation by consuming excess CPU time, copying itself to other programs, and working to destroy

disk files. The virus program can only start the infection process when someone unwittingly chooses to execute the program containing the virus.

A *computer worm* is similar to a computer virus except that it does not integrate its code into other programs. A worm is an independent program that requires someone to execute the program to begin propagating itself across a computer network. The “I Love You” virus that created havoc in 2000 was a mixture of a worm and a virus. The “I Love You” malware started the infection process by duping the email recipient into believing they would discover who sent the anonymous flirtation by executing the email’s attachment. Upon execution it worked like a virus by infecting programs with code that would replicate itself when the programs were executed. The worm characteristic of “I Love You” was how it exploited a flaw in Microsoft’s Outlook email program to send copies of itself across networks to everyone listed in the user’s address book. By mixing these characteristics, the “I Love You” virus was very difficult to remove from an infected computer since it attached itself to several different executable files and it propagated quickly across the Internet to other computers by using the email flaw.

A *Trojan horse* is a program that appears to be an innocent program, such as a game or demonstration of a business application, but is really something that has malicious functionality. By tricking the user to execute the program, the Trojan horse can begin its dirty work by deleting files or consuming all the available system resources. Malware that hogs the computer’s CPU and memory resources is called a *rabbit*. A Trojan horse can easily by used as vector for starting a computer virus or computer worm infection.

Spyware is computer program that secretly collects private information such as passwords and Internet usage patterns and sending them over the Internet to a criminal hacker. Spyware programs can be propagated through computer worms, Trojan horses, or websites that require the user to install software to access web content. Once installed the spyware program can begin to create a variety of problems besides simply collecting private information. A variant of spyware is called *adware*. An adware program will flood the computer with "pop-up" advertisements from the Internet. Both spyware and adware can make a computer unusable by consuming excess computer and network resources.

The derelict programmers that create malware are constantly creating new variations on these malware themes by combing different infection vectors and infection consequences. Most malware infections require an initial program execution to start the infection process but some malware programmers have discovered how to infect computers by exploiting flaws in the computer operating systems and service programs like Web servers. The "Code Red" worm operates by exploiting a flaw in Microsoft's Web server product called Internet Information Server (IIS). The "Code Red" worm did not require a computer user to execute the malicious code to infect the system. Instead, the "Code Red" worm scans the Internet looking for systems running IIS. When it finds an IIS service, it attacks by exploiting flaw called *buffer overflow* to override the normal operation of the IIS software and infect the computer system. A buffer overflow attack works by overloading the memory space a program uses for execution. A malicious programmer can exploit this problem by overloading the program buffer and inserting program execution statements of their own to hijack the operation of the computer. When

the computer is infected with the “Code Red” worm, it starts scanning the Internet for more computers running IIS to infect. The “Code Red” infected computer will also perform other date-triggered activities such as flooding popular web servers, like Microsoft’s main web site, with meaningless requests to create a *denial of service attack*. Denial of service attacks can seriously interrupt business activity by making it impossible for computer systems to operate properly. The financial impacts of any type of computer infection can be very serious considering the business critical nature of the computer service that the infection disrupts.

Malware Protection

Defending against malware infections requires constant diligence. Installing anti-virus software is a good first line of defense for a business owner. There are many commercially available anti-virus programs from companies like Symantec, McAfee, and Kaspersky. These companies compete by staying up to date on the latest malware attack methods and quickly developing countermeasures. Since hackers are constantly changing their methods, anti-virus vendors must constantly develop defense solutions. A business owner must be diligent in receiving and installing these updates to the anti-virus software. The update process for should be automated, but the business owner must still regularly check to make sure the anti-virus protection process is working properly. There are freely available anti-virus programs, such as AVG from Grisoft, Inc. (http://free.grisoft.com) and BitDefender (http://www.bitdefender.com), but a business owner needs to be aware that most free anti-virus products have limitations that may force them to use professional grade solutions that require licensing for business use. Simply put, you get what you pay

for, and the free products may not protect against the most current forms of malware and usually require more manual work from the user to keep virus protection up to date.

In addition to anti-virus software it also is advisable to install spyware protection software. Commercially available anti-virus solutions are getting better at including spyware protection but the pace of change for spyware threats is greater than attacks from virus, worms and other forms of malware. A business owner may need to install additional spyware protection software to cover the gaps between what their anti-virus solution provides and the spyware threats that exist on the Internet. A freely available program called Spybot Search & Destroy is a very popular spyware detection, removal, and protection application that does an excellent job of stopping spyware infections. Spyware S&D also provides automated spyware definition updates to make it easy to keep computers protected from the latest spyware threats.

Running a combination of anti-virus and anti-spyware software can be a very effective front-line defense against malware attacks. Running these programs will impact a computer's performance but they are designed to minimize the drain on computer resources and their benefits far outweigh the risks of not protecting the computer.

Another step towards fortifying business computers from malware attacks can be achieved by scanning incoming emails for messages containing malware attachments. Since email is a widely used vector for propagating malware, it makes sense to focus attention at this particular point of attack. If a business uses computers dedicated as email servers they can install anti-virus software that scans all inbound and outbound messages for attachments that contain malware. This removes the threat of attacks reaching other computers used by a business. By running a very simple filter that removes attachments

that are executable files, such as files with .exe, .vbs, and .jse extensions, on email servers, the business can achieve a highly effective email scanning solution for free. It is very rare that a business oriented email will have an executable file as an email attachment so must attachments of this type are suspicious. The “I Love You” virus was spread as a Visual Basic script (.vbs) attachment and by that very nature it was suspicious so some people refused to run the attached file. Unfortunately, many more people did not notice the file type or did not trust their suspicions and executed the attachment. A simple filter at the email server would have eliminated the threat of the “I Love You” bug before it ever reached the intended victim’s email in-box.

In the rare case that there is a legitimate need to send and receive executable file types as attachments in emails, a business owner can temporarily suspend the filter or make other arrangements to receive the file. This minor inconvenience far outweighs the benefits that email filtering provides for preventing malware attacks.

Most business owners understand the need for anti-virus software but given the rate that malware still creates business interruptions it is clear that there still exists gaps in the solutions that they may have in place. If a business does not have anti-malware software running then it is simply waiting for an attack to cause problems. A prudent business owner will schedule time to run security audits to check that anti-malware software is installed, that the threat definitions for the software are up to date, and that the software is running properly on all business systems. A quarterly inventory and review of computer systems can be a good time to perform for system security audits. The scheduled security reviews should also check that all the latest software patches from software vendors are in place. Hacker’s are constantly discovering new security flaws in

operating systems and other software applications. Software vendors like Microsoft provide software patches that correct these problems free of charge. The software flaws that the “I Love You” and “Code Red” bugs exploited have been remedied with patches from Microsoft, but they are no good if they are not installed. A regularly scheduled security audit can also serve as a good time to communicate computer usage policies to employees. Communicating the security motivations for policies about installing personal software and other activities that can compromise business information security works to employees helps to reinforce their responsibilities towards protecting company computer systems.

Staying current on new malware threats is also very important. The convenience and speed that communication occurs with the Internet also creates an environment that hackers use to share information on exploits. This speed can create a window of opportunity for hackers called a “zero-day exploit.” This is an exploit that works against a newly discovered software flaw on the very day that the vulnerability becomes general public knowledge. The threat from a zero-day attack is critical because it works to take advantage of the time lag between discovery of a flaw and when a patch to fix the flaw becomes available. The zero-day attack threat requires a business manager to stay aware of current security issues and to understand what counter-measures could be put in place to minimize the risks from a zero-day exploit. One simple step a business manager can take to stay current on computer security issues is to sign up to receive security alerts from the U.S. Department of Homeland Security’s Computer Emergency Readiness Team (US-CERT). The US-CERT office provides very useful information about current vulnerabilities, security threats, and exploits. These alerts are sent automatically to

anyone who registers at the US-CERT website, http://www.us-cert.gov/cas/techalerts/index.html.

A business owner can greatly minimize the risks that malware attacks present to business productivity by following four steps:

1. Installing software to counter the threats from malware.
2. Regularly checking computer systems to make sure they are up to date with all patches and malware definitions.
3. Stays informed about new information security threats.
4. Communicate computer usage policies and threat awareness to employees.

The next area of focus that can further secure business information systems is the computer network and the business network connection to the Internet.

Network Protection

Any small or medium sized business that uses computers will almost certainly need to network the computers together to make the most effective use of the computer's capabilities to share and process business information. Today's modern business environment makes connecting business computers to the Internet almost a certain requirement. This means that protecting the business computer network from attacks from hackers is a primary concern to the business owner interested in securing business information and productivity. The Internet is predominantly the biggest source of threats to computer security and therefore connections to the Internet need to be monitored and secured.

The first line of network defense is a firewall. The firewall is a network router that can filter networking packets based upon the type of information they carry. The firewall sets the perimeter barrier between the business computer network and the Internet. The Internet provider to a business is typically a phone company or cable company. They will provide a basic connection to the Internet and may promise some degree of network security but the business owner still should take steps by placing a network firewall between the Internet provider's demarcation point and the business computer network. This effectively blinds the Internet to the internal business computer network configuration. The firewall gives control over the types of information packets that can flow in to and out of the business computer network.

Managing computer networking equipment like routers and firewalls requires a high degree of training and skill so it is not likely the business owner would directly be

managing this equipment, however it is important that they understand some basic terminology and the functions that the equipment provides.

The basic wired computer network can be effectively protected by the network firewall. To further the protection, a business owner can install a software firewall on each of the business computers. A freely available software firewall called ZoneAlarm from Zone Labs (http://www.zonelabs.com) can help further strengthen a business network defense plan.

If the business owner chooses to take advantage of wireless networking then they need to be very aware of how they can greatly increase the chances of an intruder breaching network security and gaining access to the business computer network. Wire networks have the security benefits of being protected from physical intrusions by the fact that they exist in facilities that can be locked. If the business controls access to the building then they control the physical integrity of the wired network. Wireless networks eliminate this physical layer of protection because they broadcast all network traffic using radio frequencies. Anyone with the proper radio receiver can intercept the radio signals broadcasting all network traffic.

The first generation of wireless networking technology that was commercially available, called 802.11b, tried to implement a security feature called Wireless Encryption Protocol (WEP). This protocol encrypts the data transmissions to prevent intruders for intercepting the network traffic. Unfortunately, the encryption algorithms used by WEP are not very strong and it was quickly discovered that they could be easily cracked with some very simple radio technology and widely available networking packet processing software. If a business owner has an 802.11b wireless network installed, they

should seriously considered upgrading to the latest generation of wireless network equipment, 802.11g, which uses a new encryption protocol called Wi-Fi Protected Access (WPA). WPA technology is currently not subject to encryption cracking problems and the Institute of Electrical and Electronics Engineers (IEEE) Standards committee responsible for the 802.11g standard is continuously reviewing and upgrading the technology to make it even more secure.

If the business does implement a wireless network then it should follow some basic steps to secure the system. The first step is to change the default passwords that come on vendor networking equipment. Hacker's know these passwords and it is the first thing they will check to try and crack both wire and wireless networks. The next step is to enable the wireless encryption security feature. Wireless systems do not come with the feature enabled by default. It is very easy to simply plug in the wireless networking components and start connecting computers over the air. The only problem is that by doing this using the default configuration leaves the wireless computer network wide open to attack. Anyone that can pick up the network broadcast can intercept every bit of network traffic. The third step is to disable the Service Set Identifier (SSID) broadcast feature. The SSID is the name used to identify the wireless network. The wireless equipment comes with a default name and broadcast turned on by default to make initial installation of the wireless network easy. Public Wi-Fi hotspots use the SSID to make their service available. Private businesses should not be broadcasting this identity because it makes it easier for hackers to find the business wireless network. Following these simple steps can change a wireless network from a large computer security risk to a valuable business productivity tool.

Network Intrusion Detection

A business owner should also consider implementing a network Intrusion Detection System. These systems work to identify network traffic that could be associated with an attempt to break into a computer network. There are two basic types of IDS that search for intrusion activity. The first type is called *signature-based* IDS and it operates by performing simple pattern-matching to find network activity that is associated with a known type of network attack. The second type is called anomaly based or heuristic IDS and it operates by building a model of normal network traffic and then flags activity that is different and could be associated with an attack. The heuristic type of IDS is the most sophisticated and requires training the model and a higher level of interactive management than the signature-based IDS. By implementing either type of IDS the business owner effectively puts up the radar to become aware of attempts to probe and illicitly access the business computer network. This is good information for anyone concerned about computer network security.

Information Backups, Business Continuity, and Disaster Recovery

Besides all the malicious threats that can destroy and damage business information, there are the normal inadvertent human errors, hardware failures and variety of natural disasters that can cause data loss and put the business operations in jeopardy. Regardless of the root cause for a business data loss event, the business manager will need to have a plan in place to recover the data, restore it, and continue business operation. Anyone who uses a computer and stores valuable data on the system needs to backup up the data to protect it from loss. Beyond the simple process of backing up and restoring business data, a company must consider the consequences of having the business data and computer systems unavailable for any period of time. The company must have a plan for how it will recover from a variety of scenarios that could interrupt the business' ability to operate.

Information Backups and Restores

Basic common computer operations require the ability to backup all data on computer systems. The technology that can be employed to backup data varies widely and the choices in technology will depend on the speed the backup system operates and the costs associated with running the backup system. The first deciding factor in choosing a backup system is to evaluate the volume of data contained on business computers and the timeframes available for backing up the data. Typically backups occur after normal business hours so they do not interfere with computer performance. The challenge for the backup system is that it must copy and store all business data to backup media in a defined time window. If the data volume becomes too large and the backup system operates too slowly, then the backups will not be complete by the time a business begins

the next cycle of operations. The next consideration that business must examine for its backup procedures is how long it will take to recover a data set in the event of a data loss. Business data sets may have different levels of business importance so the business manager may need to categorize and prioritize how data sets are backed up so that the most critical data sets have the fastest recovery times. Finally, consideration needs to be paid to the importance of storing copies of the backups in a different location from where the normal business computer operations occur. Off-site storage of data backups is required for the ability to recover from a disaster that would destroy the primary business site. Data loss events range from the accidental deletion of a file to the complete destruction the business location and all business equipment. The data recovery strategies must range to match the most typical data loss events to the most disastrous ones.

Business Continuity

When a data loss event occurs the business must have a plan to recover and continue business operations. Business Continuity Planning deals with addressing the range of data loss scenarios that can affect a company. The company ideally needs to have a set of plans and procedures to address simple data loss of a few files due to an accidental deletion, to a hardware failure that could make some data sets and computer applications unavailable for a period of time, to a complete loss of business systems. Each of these scenarios could require a different strategy to address the business impact and expected time to implement a full recovery. Restoring a few files might only take an hour to recover from a backup, but rebuilding an entire file or application server could take several days. If the business can not afford to be with out the computer system for that time period then it needs to consider implementing a redundant hardware solution to

mitigate the risk of catastrophic hardware failure. Simple cost benefit analysis will reveal when the costs to implement a redundant system outweigh the losses the business could accrue if the computer system is unavailable for a specified length of time. Applying this type of analysis to the types of problems that can result in computer operations will help identify the best strategies to mitigate the risks to the business. A business that does not have plans to recover quickly from any situation that can interrupt business operations is simply asking for trouble.

Disaster Recovery

A special category of business continuity planning involves how the business will recover from a catastrophic event that can make operating its normal business facilities impossible. Fires, floods, hurricanes, earthquakes, and terrorist attacks appear in the news all the time but they are rare events with significant consequences to business operations. A company without a plan on how to restart operations in a new location in a timely manner can literally be wiped out by a disaster.

Most small and medium sized companies probably do not have the capital to spend on minimizing the impact of a disaster so that it can restart operations in a few days. The company still should consider how it would go about the process of rebuilding. Disaster recovery planning for computer systems involves making an inventory of all types of equipment and software necessary to restart the business in a new location. A company that exercises good backup procedures and stores business data sets in an off-site location can leverage these backups to restart business activity. The off-site storage location should also have copies of all software installation media and all instructions for rebuilding computer systems once new computer hardware become available.

The best way to test business continuity and disaster recovery plans is to run drills that test the ability of the people, plans, and materials to adequately recover from events in the desired length of time. These tests should reveal where procedures need to be updated and weaknesses in recovery skills. Simply having plans for addressing events that will interrupt business activity is not a guarantee that they will work when the time arrives. Stress levels on people will rise when an actual recovery scenario occurs. The best way to minimize the impact on people is to practice the recovery procedures on a regular basis so they have confidence that they have the right skills and materials to get the job done.

Conclusions and Recommendations

Information Security is a just as important to small and medium sized business as it is to large corporations and institutions. The risk to small and medium sized businesses is much higher given that a event that interrupts business activity and causes cash losses are not as easy to absorb by small companies. This problem is compounded by smaller companies having fewer resources to devote to securing their information systems. This means that small and medium sized business operators must be aware of the risks to their computer systems and business information. They must be aware of the basic approaches to mitigating these risks. This field project has been an effort to document these risks and the approaches that are in reach of even the smallest business operators.

Awareness of the terminology surrounding information security is an important first step towards being able to better manage the computer systems that are vital to a business operation. Knowledge of the terms and some basics resources for assistance in

mitigating risks can go a long way to preventing the most basic attacks. It is unrealistic to believe that all risks to information security can be eliminated but it is possible to greatly reduce the risks from the most common threats.

Simply understanding how to articulate and implement good password policies reduces the easiest way to lose control of business computing data and services. Being aware of the tricks that criminals will play to social engineer their way into accessing a company computer can help better identify suspicious activities. Diligently updating application software patches and malware detection software are the best ways to prevent the damage malware attacks can cause to business data and service availability. This includes staying up to date on the latest computer security threats circulating in the wild on the Internet. Putting up a basic network firewall and intrusion detection system quickly shuts the door to some of the most difficult computer attacks a company could face. Finally, establishing an appropriate set of business continuity plans supported by a system that can backup all the company's data can greatly reduce the impact of all types of data loss and system unavailability events. Disaster recovery is not a daily occurrence but understanding what it would take to rebuild the computer systems that support business activity keep the business management aware of how healthy their information security policies and procedures are functioning. All risks to business operations can not be eliminated but knowledge of the easiest places to mitigate risks can work to greatly reduce the chances of small problems escalating to massive failures that challenge the business' ability to survive.

Additional research that surveys small and medium sized businesses would reveal where SMBs have the most difficulty in dealing with information security. Understanding

these issues can help to better the framework as an aid for SMBs working to address information security in their organizations. Another area of useful research would be the topic of computer security testing. This topic focuses on test methods and security monitoring that can help reveal computer security problems that could be exploited. Monitoring provides awareness of potential hacking activity and this provides business management with ability to immediately address the threat before there is a compromise in security.

Appendix I: References

Carnegie Mellon Software Engineering Institute, CERT Coordination Center, "Securing Desktop Workstations," Available from Internet: http://www.cert.org/security-improvement/practices/p034.html (accessed 3/20/2006).

Danchev, Dancho, WindowSecurity.com, "Passwords - Common Attacks and Possible Solutions," Jan 07, 2005, Available from Internet: http://www.windowsecurity.com/articles/Passwords-Attacks-Solutions.html (accessed 3/20/2006).

Department of Homeland Security: Information Analysis Infrastructure Protection, National Infrastructure Protection Center, "Seven Simple Computer Security Tips For Small Business and Home Computer Users," Available from Internet: http://webharvest.gov/peth04/20041020071037/www.nipc.gov/publications/nipcpub/computertips.htm (accessed 3/20/2006).

Kabay, Michael E., "The NCSA Guide to Enterprise Security: Protecting Information Assets," McGraw-Hill (1996).

Lemos, Rob, CNET News.com, "Passwords: The Weakest Link?" May 22, 2002, Available from Internet: http://news.com.com/2009-1001-916719.html (accessed 3/20/2006).

Mansfield, Tony, Kelly, Gavin, Chandler, David, and Kane, Jan, National Physical Laboratory UK, "Biometric Product Testing Final Report, Issue 1.0," March 19, 2001 Available from Internet: http://www.cesg.gov.uk/site/ast/biometrics/media/BiometricTestReportpt1.pdf (accessed 3/20/2006).

Mansfield, Tony, Centre for Mathematics and Scientific Computing, National Physical Laboratory UK, "Biometric authentication in the real world," Available from Internet: http://www.publicservice.co.uk/pdf/home_office/autumn2001/p36.pdf (accessed 3/20/2006).

McGill University, Network and Communications Services, "Understanding passwords," March 03, 2006, ~~Available from Internet~~: http://www.mcgill.ca/ncs/products/security/understandpass/ (accessed 3/20/2006). This information is no longer available on the Internet (6/4/2009).

Microsoft Technet, "Step-by-Step Guide to Enforcing Strong Password Policies," Available from Internet: http://www.microsoft.com/technet/prodtechnol/windowsserver2003/technologies/directory/activedirectory/stepbystep/strngpw.mspx (accessed 3/20/2006).

Mitnick, Kevin, SecurityFocus, “My first RSA Conference,” April 30, 2004, Available from Internet: http://www.securityfocus.com/news/199 (accessed 3/20/2006).

Nelson, Rick, “Methods of Hacking: Social Engineering,” Available from Internet: http://vvv.snugg.net/security/dokumentation/dokumentation/soceng/socialeng.html (accessed 3/20/2006).

Pfleeger, Charles, and Pfleeger, Shari Lawrence, “Security in Computing,” third edition, Prentice Hall Professional Technical Reference (2003).

Proctor, Paul E., “The Practical Intrusion Detection Handbook,” Prentice Hall Professional Technical Reference (2001).

Rose, Kevin, G4TV.com, “Dark Tip: Windows Password Hacking,” February 25, 2004, Available from Internet: http://www.g4tv.com/screensavers/features/664/Dark_Tip_Windows_Password_Hacking.html (accessed 3/20/2006).

The SANS Institute, “The SANS Security Policy Project,” Available from Internet: http://www.sans.org/resources/policies/ (accessed 3/20/2006).

Salomon, David, “Data Privacy and Security,” Springer-Verlag New York, Inc. (2003).

Scambray, Joel, McClure, Stuart, and Kurtz, George, “Hacking Exposed: Network Security Secrets & Solutions,” second edition, Osbourne/McGraw-Hill (2001).

Shaffer, George, GeodSoft.com, “Good and Bad Passwords How-To,” Available from Internet: http://geodsoft.com/howto/password/cracking_passwords.htm (accessed 6/4/2009).

Stamp, Mark, “Information Security Principles and Practices,” Wiley-Interscience (2006).

Zeller, Tom Jr., The New York Times, “Black Market in Stolen Credit Card Data Thrives on Internet,” June 21, 2005, Available from Internet: http://www.nytimes.com/2005/06/21/technology/21data.html?ei=5088&en=c06809aa240685f8&ex=1277006400&partner=rssnyt&emc=rss&pagewanted=all (accessed 3/20/2006)

Appendix II: Acceptable Use Policy

This Acceptable Use Policy example is from the SANS Security Policy Project.

http://www.sans.org/resources/policies/Acceptable_Use_Policy.pdf

Note: InfoSec is an abbreviation used to designate the companies Information Security Authority.

InfoSec Acceptable Use Policy

1.0 Overview

InfoSec's intentions for publishing an Acceptable Use Policy are not to impose restrictions that are contrary to <Company Name> established culture of openness, trust and integrity. InfoSec is committed to protecting <Company Name>'s employees, partners and the company from illegal or damaging actions by individuals, either knowingly or unknowingly. Internet/Intranet/Extranet-related systems, including but not limited to computer equipment, software, operating systems, storage media, network accounts providing electronic mail, WWW browsing, and FTP, are the property of <Company Name>. These systems are to be used for business purposes in serving the interests of the company, and of our clients and customers in the course of normal operations. Please review Human Resources policies for further details. Effective security is a team effort involving the participation and support of every <Company Name> employee and affiliate who deals with information and/or information systems. It is the responsibility of every computer user to know these guidelines, and to conduct their activities accordingly.

2.0 Purpose

The purpose of this policy is to outline the acceptable use of computer equipment at <Company Name>. These rules are in place to protect the employee and <Company Name>. Inappropriate use exposes <Company Name> to risks including virus attacks, compromise of network systems and services, and legal issues.

3.0 Scope

This policy applies to employees, contractors, consultants, temporaries, and other workers at <Company Name>, including all personnel affiliated with third parties. This policy applies to all equipment that is owned or leased by <Company Name>.

4.0 Policy

4.1 General Use and Ownership

1. While <Company Name>'s network administration desires to provide a reasonable level of privacy, users should be aware that the data they create on the corporate systems remains the property of <Company Name>. Because of the need to protect <Company Name>'s network, management cannot guarantee the confidentiality of information stored on any network device belonging to <Company Name>.

2. Employees are responsible for exercising good judgment regarding the reasonableness of personal use. Individual departments are responsible for creating guidelines concerning personal use of Internet/Intranet/Extranet systems. In the absence of such policies, employees should be guided by departmental policies on personal use, and if there is any uncertainty, employees should consult their supervisor or manager.

3. InfoSec recommends that any information that users consider sensitive or vulnerable be encrypted. For guidelines on information classification, see InfoSec's Information

Sensitivity Policy. For guidelines on encrypting email and documents, go to InfoSec's Awareness Initiative.

4. For security and network maintenance purposes, authorized individuals within <Company Name> may monitor equipment, systems and network traffic at any time, per InfoSec's Audit Policy.

5. <Company Name> reserves the right to audit networks and systems on a periodic basis to ensure compliance with this policy.

4.2 Security and Proprietary Information

1. The user interface for information contained on Internet/Intranet/Extranet-related systems should be classified as either confidential or not confidential, as defined by corporate confidentiality guidelines, details of which can be found in Human Resources policies. Examples of confidential information include but are not limited to: company private, corporate strategies, competitor sensitive, trade secrets, specifications, customer lists, and research data. Employees should take all necessary steps to prevent unauthorized access to this information.

2. Keep passwords secure and do not share accounts. Authorized users are responsible for the security of their passwords and accounts. System level passwords should be changed quarterly; user level passwords should be changed every six months.

3. All PCs, laptops and workstations should be secured with a password-protected screensaver with the automatic activation feature set at 10 minutes or less, or by logging-off (control-alt-delete for Win2K users) when the host will be unattended.

4. Use encryption of information in compliance with InfoSec's Acceptable Encryption Use policy.

5. Because information contained on portable computers is especially vulnerable, special care should be exercised. Protect laptops in accordance with the .Laptop Security Tips.

6. Postings by employees from a <Company Name> email address to newsgroups should contain a disclaimer stating that the opinions expressed are strictly their own and not necessarily those of <Company Name>, unless posting is in the course of business duties.

7. All hosts used by the employee that are connected to the <Company Name> Internet/Intranet/Extranet, whether owned by the employee or <Company Name>, shall be continually executing approved virus-scanning software with a current virus database. Unless overridden by departmental or group policy.

8. Employees must use extreme caution when opening e-mail attachments received from unknown senders, which may contain viruses, e-mail bombs, or Trojan horse code.

4.3. Unacceptable Use

The following activities are, in general, prohibited. Employees may be exempted from these restrictions during the course of their legitimate job responsibilities (e.g., systems administration staff may have a need to disable the network access of a host if that host is disrupting production services). Under no circumstances is an employee of <Company Name> authorized to engage in any activity that is illegal under local, state, federal or international law while utilizing <Company Name>-owned resources. The lists below are by no means exhaustive, but attempt to provide a framework for activities which fall into the category of unacceptable use.

System and Network Activities

The following activities are strictly prohibited, with no exceptions:

1. Violations of the rights of any person or company protected by copyright, trade secret, patent or other intellectual property, or similar laws or regulations, including, but not limited to, the installation or distribution of "pirated" or other software products that are not appropriately licensed for use by <Company Name>.

2. Unauthorized copying of copyrighted material including, but not limited to, digitization and distribution of photographs from magazines, books or other copyrighted sources, copyrighted music, and the installation of any copyrighted software for which <Company Name> or the end user does not have an active license is strictly prohibited.

3. Exporting software, technical information, encryption software or technology, in violation of international or regional export control laws, is illegal. The appropriate management should be consulted prior to export of any material that is in question.

4. Introduction of malicious programs into the network or server (e.g., viruses, worms, Trojan horses, e-mail bombs, etc.).

5. Revealing your account password to others or allowing use of your account by others. This includes family and other household members when work is being done at home.

6. Using a <Company Name> computing asset to actively engage in procuring or transmitting material that is in violation of sexual harassment or hostile workplace laws in the user’s local jurisdiction.

7. Making fraudulent offers of products, items, or services originating from any <Company Name> account.

8. Making statements about warranty, expressly or implied, unless it is a part of normal job duties.

9. Effecting security breaches or disruptions of network communication. Security breaches include, but are not limited to, accessing data of which the employee is not an intended recipient or logging into a server or account that the employee is not expressly authorized to access, unless these duties are within the scope of regular duties. For purposes of this section, "disruption" includes, but is not limited to, network sniffing, pinged floods, packet spoofing, denial of service, and forged routing information for malicious purposes.

10. Port scanning or security scanning is expressly prohibited unless prior notification to InfoSec is made.

11. Executing any form of network monitoring which will intercept data not intended for the employee's host, unless this activity is a part of the employee's normal job/duty.

12. Circumventing user authentication or security of any host, network or account.

13. Interfering with or denying service to any user other than the employee's host (for example, denial of service attack).

14. Using any program/script/command, or sending messages of any kind, with the intent to interfere with, or disable, a user's terminal session, via any means, locally or via the Internet/Intranet/Extranet.

15. Providing information about, or lists of, <Company Name> employees to parties outside <Company Name>.

Email and Communications Activities

1. Sending unsolicited email messages, including the sending of "junk mail" or other advertising material to individuals who did not specifically request such material (email spam).

2. Any form of harassment via email, telephone or paging, whether through language, frequency, or size of messages.

3. Unauthorized use, or forging, of email header information.

4. Solicitation of email for any other email address, other than that of the poster's account, with the intent to harass or to collect replies.

5. Creating or forwarding "chain letters", "Ponzi" or other "pyramid" schemes of any type.

6. Use of unsolicited email originating from within <Company Name>'s networks of other Internet/Intranet/Extranet service providers on behalf of, or to advertise, any service hosted by <Company Name> or connected via <Company Name>'s network.

7. Posting the same or similar non-business-related messages to large numbers of Usenet newsgroups (newsgroup spam).

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Term	**Definition**
Spam	Unauthorized and/or unsolicited electronic mass mailings.

7.0 Revision History

Appendix III: Password Policy

This Password Policy example is from the SANS Security Policy Project.

http://www.sans.org/resources/policies/Password_Policy.pdf

Note: InfoSec is an abbreviation used to designate the companies Information Security Authority.

Password Policy

1.0 Overview

Passwords are an important aspect of computer security. They are the front line of protection for user accounts. A poorly chosen password may result in the compromise of <Company Name>'s entire corporate network. As such, all <Company Name> employees (including contractors and vendors with access to <Company Name> systems) are responsible for taking the appropriate steps, as outlined below, to select and secure their passwords.

2.0 Purpose

The purpose of this policy is to establish a standard for creation of strong passwords, the protection of those passwords, and the frequency of change.

3.0 Scope

The scope of this policy includes all personnel who have or are responsible for an account (or any form of access that supports or requires a password) on any system that resides at any <Company Name> facility, has access to the <Company Name> network, or stores any non-public <Company Name> information.

4.0 Policy

4.1 General

• All system-level passwords (e.g., root, enable, NT admin, application administration accounts, etc.) must be changed on at least a quarterly basis.

• All production system-level passwords must be part of the InfoSec administered global password management database.

• All user-level passwords (e.g., email, web, desktop computer, etc.) must be changed at least every six months. The recommended change interval is every four months.

• User accounts that have system-level privileges granted through group memberships or programs such as "sudo" must have a unique password from all other accounts held by that user.

• Passwords must not be inserted into email messages or other forms of electronic communication.

• Where SNMP is used, the community strings must be defined as something other than the standard defaults of "public," "private" and "system" and must be different from the passwords used to log in interactively. A keyed hash must be used where available (e.g., SNMPv2).

• All user-level and system-level passwords must conform to the guidelines described below.

4.2 Guidelines

A. General Password Construction Guidelines

Passwords are used for various purposes at <Company Name>. Some of the more common uses include: user level accounts, web accounts, email accounts, screen saver protection, voicemail password, and local router logins. Since very few systems have

support for one-time tokens (i.e., dynamic passwords which are only used once), everyone should be aware of how to select strong passwords.

Poor, weak passwords have the following characteristics:

• The password contains less than eight characters

• The password is a word found in a dictionary (English or foreign)

• The password is a common usage word such as:

  - o Names of family, pets, friends, co-workers, fantasy characters, etc.
  - o Computer terms and names, commands, sites, companies, hardware, software.
  - o The words "<Company Name>", "sanjose", "sanfran" or any derivation.
  - o Birthdays and other personal information such as addresses and phone numbers.
  - o Word or number patterns like aaabbb, qwerty, zyxwvuts, 123321, etc.
  - o Any of the above spelled backwards.
  - o Any of the above preceded or followed by a digit (e.g., secret1, 1secret)

Strong passwords have the following characteristics:

• Contain both upper and lower case characters (e.g., a-z, A-Z)

• Have digits and punctuation characters as well as letters e.g., 0-9, !@#$%^&*()_+|~-=\‘{}[]:";’<>?,./)

• Are at least eight alphanumeric characters long.

• Are not a word in any language, slang, dialect, jargon, etc.

• Are not based on personal information, names of family, etc.

• Passwords should never be written down or stored on-line. Try to create passwords that can be easily remembered. One way to do this is create a password based on a song title,

affirmation, or other phrase. For example, the phrase might be: "This May Be One Way To Remember" and the password could be: "TmB1w2R!" or "Tmb1W>r~" or some other variation.

NOTE: Do not use either of these examples as passwords!

B. Password Protection Standards

Do not use the same password for <Company Name> accounts as for other non-<Company Name> access (e.g., personal ISP account, option trading, benefits, etc.).

Where possible, don't use the same password for various <Company Name> access needs. For example, select one password for the Engineering systems and a separate password for IT systems. Also, select a separate password to be used for an NT account and a UNIX account.

Do not share <Company Name> passwords with anyone, including administrative assistants or secretaries. All passwords are to be treated as sensitive, Confidential <Company Name> information.

Here is a list of "dont's":

• Don't reveal a password over the phone to ANYONE

• Don't reveal a password in an email message

• Don't reveal a password to the boss

• Don't talk about a password in front of others

• Don't hint at the format of a password (e.g., "my family name")

• Don't reveal a password on questionnaires or security forms

• Don't share a password with family members

• Don't reveal a password to co-workers while on vacation

If someone demands a password, refer them to this document or have them call someone in the Information Security Department.

Do not use the "Remember Password" feature of applications (e.g., Eudora, OutLook, Netscape Messenger).

Again, do not write passwords down and store them anywhere in your office. Do not store passwords in a file on ANY computer system (including Palm Pilots or similar devices) without encryption. Change passwords at least once every six months (except system-level passwords which must be changed quarterly). The recommended change interval is every four months. If an account or password is suspected to have been compromised, report the incident to InfoSec and change all passwords.

Password cracking or guessing may be performed on a periodic or random basis by InfoSec or its delegates. If a password is guessed or cracked during one of these scans, the user will be required to change it.

C. Application Development Standards

Application developers must ensure their programs contain the following security precautions.

Applications:

• should support authentication of individual users, not groups.

• should not store passwords in clear text or in any easily reversible form.

• should provide for some sort of role management, such that one user can take over the functions of another without having to know the other’s password.

• should support TACACS+ , RADIU.S. and/or X.509 with LDAP security retrieval, wherever possible.

D. Use of Passwords and Passphrases for Remote Access Users

Access to the <Company Name> Networks via remote access is to be controlled using either a one-time password authentication or a public/private key system with a strong passphrase.

E. Passphrases

Passphrases are generally used for public/private key authentication. A public/private key system defines a mathematical relationship between the public key that is known by all, and the private key, that is known only to the user. Without the passphrase to "unlock" the private key, the user cannot gain access.

Passphrases are not the same as passwords. A passphrase is a longer version of a password and is, therefore, more secure. A passphrase is typically composed of multiple words. Because of this, a passphrase is more secure against "dictionary attacks."

A good passphrase is relatively long and contains a combination of upper and lowercase letters and numeric and punctuation characters. An example of a good passphrase:

"The*?#>*@TrafficOnThe101Was*&#!#ThisMorning"

All of the rules above that apply to passwords apply to passphrases.

5.0 Enforcement

Any employee found to have violated this policy may be subject to disciplinary action, up to and including termination of employment.

6.0 Definitions

Terms	Definitions
Application Administration Account	Any account that is for the administration of an application (e.g., Oracle database administrator, ISSU administrator).

7.0 Revision History